

09-11-00

A

Please type a plus sign (+) inside this box → ☒

Approved for use through 09/30/2000 OMB 0651-0032
Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

| | | |
|--|--|-------------------------|
| UTILITY PATENT APPLICATION TRANSMITTAL <small>(Only for new nonprovisional applications under 37 C.F.R. § 1.53(b))</small> | Attorney Docket No. | 28197.3.02 |
| | First Inventor or Application Identifier | Aureliano Tan, Jr. |
| | Title | DIGITAL IDENTITY DEVICE |
| | Express Mail Label No. | EL262829098US |

| | |
|---|---|
| APPLICATION ELEMENTS <small>See MPEP chapter 600 concerning utility patent application contents.</small> | ADDRESS TO: Assistant Commissioner for Patents Box Patent Application Washington, DC 20231 |
| 1. <input checked="" type="checkbox"/> * Fee Transmittal Form (e.g., PTO/SB/17) <small>(Submit an original and a duplicate for fee processing)</small> 2. <input checked="" type="checkbox"/> Specification [Total Pages 32] <small>(preferred arrangement set forth below)</small> - Descriptive title of the Invention - Cross References to Related Applications - Statement Regarding Fed sponsored R & D - Reference to Microfiche Appendix - Background of the Invention - Brief Summary of the Invention - Brief Description of the Drawings (if filed) - Detailed Description - Claim(s) - Abstract of the Disclosure 3. <input checked="" type="checkbox"/> Drawing(s) (35 U.S.C. 113) [Total Sheets 15] 4. Oath or Declaration [Total Pages 2] a. <input checked="" type="checkbox"/> Newly executed (original or copy) b. <input type="checkbox"/> Copy from a prior application (37 C.F.R. § 1.63(d)) <small>(for continuation/divisional with Box 16 completed)</small> i. <input type="checkbox"/> <u>DELETION OF INVENTOR(S)</u> Signed statement attached deleting inventor(s) named in the prior application, see 37 C.F.R. §§ 1.63(d)(2) and 1.33(b). | 5. <input type="checkbox"/> Microfiche Computer Program (Appendix) 6. Nucleotide and/or Amino Acid Sequence Submission (if applicable, all necessary) a. <input type="checkbox"/> Computer Readable Copy b. <input type="checkbox"/> Paper Copy (identical to computer copy) c. <input type="checkbox"/> Statement verifying identity of above copies |
| ACCOMPANYING APPLICATION PARTS | |
| 7. <input type="checkbox"/> Assignment Papers (cover sheet & document(s)) 8. <input type="checkbox"/> 37 C.F.R. § 3.73(b) Statement of Power of Attorney (when there is an assignee) 9. <input type="checkbox"/> English Translation Document (if applicable) 10. <input type="checkbox"/> Information Disclosure Statement (IDS)/PTO-1449 [Copies of IDS Citations] 11. <input type="checkbox"/> Preliminary Amendment 12. <input checked="" type="checkbox"/> Return Receipt Postcard (MPEP 503) (Should be specifically itemized) 13. <input type="checkbox"/> * Small Entity Statement filed in prior application, Status still proper and desired (PTO/SB/09-12) 14. <input type="checkbox"/> Certified Copy of Priority Document(s) (if foreign priority is claimed) 15. <input checked="" type="checkbox"/> Other: Express Mail Certificate | |
| * NOTE FOR ITEMS 1 & 13: IN ORDER TO BE ENTITLED TO PAY SMALL ENTITY FEES, A SMALL ENTITY STATEMENT IS REQUIRED (37 C.F.R. § 1.27), EXCEPT IF ONE FILED IN A PRIOR APPLICATION IS RELIED UPON (37 C.F.R. § 1.29). | |

16. If a CONTINUING APPLICATION, check appropriate box, and supply the requisite information below and in a preliminary amendment:

☐ Continuation ☐ Divisional ☐ Continuation-in-part (CIP) of prior application No: _____

Prior application information: Examiner _____ Group / Art Unit: _____

For CONTINUATION or DIVISIONAL APPS only: The entire disclosure of the prior application, from which an oath or declaration is supplied under Box 4b, is considered a part of the disclosure of the accompanying continuation or divisional application and is hereby incorporated by reference. The incorporation can only be relied upon when a portion has been inadvertently omitted from the submitted application parts.

17. CORRESPONDENCE ADDRESS

☐ Customer Number or Bar Code Label _____ or ☒ Correspondence address below

(Insert Customer No. or Attach bar code label here)

| | | | | | |
|---------|-----------------------------------|-----------|--------------|----------|--------------|
| Name | Tim Headley | | | | |
| | Haynes and Boone, L.L.P. | | | | |
| Address | 1000 Louisiana Street, Suite 4300 | | | | |
| City | Houston | State | Texas | Zip Code | 77002-5012 |
| Country | USA | Telephone | 713-547-2040 | Fax | 713-236-5526 |

| | | | |
|-------------------|--------------------|-----------------------------------|--------|
| Name (Print/Type) | Tim Headley | Registration No. (Attorney/Agent) | 31,765 |
| Signature | <i>Tim Headley</i> | Date | 9-8-00 |

Burden Hour Statement. This form is estimated to take 0.2 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Box Patent Application, Washington, DC 20231.

H-217811.2

EXPRESS MAIL LABEL NO.: **EL262829098US**

DATE OF DEPOSIT: **September 8, 2000**

I hereby certify that this paper and fee are being deposited with the United States Postal Service Express Mail Post Office to Addressee service under 37 CFR §1.10 on the date indicated above and is addressed to : Box PATENT APPLICATION, Commissioner for Patents, Washington, D.C. 20231.

Michelle Baxter

NAME OF PERSON MAILING PAPER AND FEE




SIGNATURE OF PERSON MAILING PAPER AND FEE

DIGITAL IDENTITY DEVICE

Inventor: Aureliano Tan, Jr.
Sugar Land, TX

Attorney: Tim Headley
HAYNES and BOONE, LLP
1000 Louisiana, Suite 4300
Houston, Texas 77002-5012
Tel: 713-547-2040
Fax: 713-236-5526
headleyt@haynesboone.com

| | |
|---|---|
| EXPRESS MAIL LABEL NO.: EL262829098US | DATE OF DEPOSIT: September 8, 2000 |
| I hereby certify that this paper and fee are being deposited with the United States Postal Service Express Mail Post Office to Addressee service under 37 CFR §1.10 on the date indicated above and is addressed to : Box PATENT APPLICATION, Commissioner for Patents, Washington, D.C. 20231. | |
| Michelle Baxter NAME OF PERSON MAILING PAPER AND FEE |  SIGNATURE OF PERSON MAILING PAPER AND FEE |

DIGITAL IDENTITY DEVICE

Cross Reference To Related Applications

This application claims the benefit of the filing date of United States provisional patent application Serial No. 60/179,989, filed on February 3, 2000, the disclosure of which is incorporated by reference.

Background of the Invention

The present invention relates generally to the privacy and security of digital information, and in particular to the privacy and security of electronic communication.

In electronic communication, the authentication of the parties involved is generally required. Each party should be clearly identifiable and distinguishable. The electronic communication between parties should also be secure. The parties should also be able to grant various levels of permission for access to their respective information.

What is needed is a method of identifying microprocessors and using this method of microprocessor identification in a digital identity device for entities to use in electronic communications.

Summary of the Invention

The present invention is a microprocessor identity device for use in a digital identity device. The digital identity device will contain identity information that will function with the microprocessor identity device to create a unique digital identity for all individuals or corporations.

According to one aspect of the invention, a digital identity device for identifying individuals includes a microprocessor identity device, a digital identity, and means for binding the microprocessor identity device to the digital identity.

5

According to another aspect of the invention, an apparatus for globally registering digital identity devices includes one or more digital identity devices, a database of digital identity device information, and means for communications between the digital identity devices and the database.

10

According to another aspect of the invention, a method of licensing a software program to a computer, the computer having a microprocessor containing identity information about the computer, includes the steps of starting the installation of the software program to the computer, transmitting a license key and the identity information about the computer to a central database, receiving information to bind the license key to the identity information, binding the license key to the identity information in the computer, and completing the installation.

15

20

According to another aspect of the invention, a method of licensing a software program to a computer, the computer having a microprocessor containing identity information about the computer, includes the steps of receiving a license key and the identity information about the computer into a central database, transferring a status of the license key and the identity information in the central database to the computer, accepting the license key and the identity information, and binding the license key to the identity information in the central database.

25

According to another aspect of the invention, a method of de-licensing a software program to a computer, the computer having a microprocessor containing identity information about the computer, includes starting the de-

installation of the software program to the computer, transmitting a license key and the identity information about the computer to a central database, receiving information to unbind the license key to the identity information, unbinding the license key to the identity information in the computer, and completing the reinstallation.

According to another aspect of the invention, a method of de-licensing a software program to a computer, the computer having a microprocessor containing identity information about the computer, includes receiving a license key and the identity information about the computer into a central database, transferring a status of the license key and the identity information in the central database to the computer, accepting the license key and the identity information, and unbinding the license key to the identity information in the central database.

According to another aspect of the invention, a method of tracking software usage by a computer, the computer having a microprocessor containing identity information about the computer, includes receiving a usage profile from the computer and storing the usage profile in a central database.

Brief Description of the Drawings

Fig. 1 is a schematic view illustrating an embodiment of a system for a digital identity device.

Fig. 2 is a schematic view illustrating an embodiment of the digital identity device of Fig. 1.

Fig. 3 is a schematic view illustrating an alternate embodiment of the digital identity device of Fig. 1.

Fig. 4 is a schematic view illustrating an embodiment of the microprocessor identity device of Fig. 2.

Fig. 5 is a schematic view of an alternate embodiment of the microprocessor identity device of Fig. 2.

Fig. 6 is a schematic view of an alternate embodiment of the microprocessor identity device of Fig. 2.

5 Fig. 7 is a schematic view of an embodiment of the computer card of Fig. 1.

Fig. 8 is a schematic view of an alternate embodiment of the computer card of Fig. 1.

10 Fig. 9 is a schematic view of a system for globally authenticating the digital identity devices.

Fig. 10 is a schematic view of a system for communication between one or more of the digital identity devices of Fig. 1.

Fig. 11A is a schematic view of a system for licensing software.

15 Fig. 11B is a schematic view of an alternate system for licensing software.

Fig. 12 is a schematic view of a method for licensing software, using the system of Fig. 11A.

Fig. 13 is a schematic view of a method for de-licensing software using the system of Fig. 11A.

20 Fig. 14 is a schematic view of a method for monitoring software usage using the system of Fig. 11A.

Detailed Description of the Preferred Embodiment

To assist in this detailed description a glossary of terms and acronyms follows:

25 authentication the ability of the receiver of a message to
 positively identify the author of the message
 digital signature a digital code that can be attached to an

| | | |
|----|-----------------|---|
| | | electronically transmitted message that uniquely identifies the sender |
| | e-mail | electronic mail |
| | GRID | global registry of digital identity devices |
| 5 | I/O | input/output |
| | integrity | the guarantee that a message has not changed in the process of transmission |
| | license key | an encrypted code that grants permission to use a software program on a fixed amount of computers |
| 10 | non-repudiation | the inability of the author of a message to deny sending the message |
| | NVRAM | non-volatile random access memory |
| | PCI | peripheral component interconnect |
| | PCMCIA | personal computer memory card international |
| 15 | | association |
| | PDA | personal digital assistant |
| | PROM | programmable read-only memory |
| | RISC | reduced instruction set computer |
| | UID | universal identity card |
| 20 | USB | universal serial bus |
| | VME | VersaModule Eurocard |

Referring to Fig. 1, a system 100 for digitally identifying individuals or corporations includes a digital identity device 105 (further illustrated in Fig. 2), a computer card 110, and a connection 115. The connection 115 couples the digital identity device 105 to the computer card 110.

The digital identity device 105 contains the identity information of either an individual or a corporation. The digital identity device 105 contains one or more passwords. The passwords are encrypted.

The computer card 110 contains the digital identity device 105. The computer card 110 has input/output capabilities for a connection to a separate computer. The computer card 110 is a computer board. In an alternate embodiment, the computer card 110 is a standard computer card which can be plugged to a computer bus or any computer device with an input/output port. In an alternate embodiment, the computer card 110 displays the identity information within the digital identity device 105. Some examples of the computer card 110 are a Personal Computer Memory Card International Association (PCMCIA) card, a PCI card for a personal computer, an Sbus card for a Sun Microsystems computer, a VME card, a Multibus card or any card that attaches to a Universal Serial Bus (USB), to a FireWire, or to another computer input/output (I/O) port.

The connection 115 couples the digital identity device 105 to the computer card 110. The connection 115 is solder. In an alternate embodiment, the connection 115 is connector pins. The connection 115 depends on the computer card 110 of the system 100. In an alternate embodiment, the digital identity device 105 is also soldered to other discrete components on a printed circuit of the computer card 110.

In an alternate embodiment, the digital identity device 105 is a Universal Serial Bus (USB) device. The connection 115 couples the digital identity device 105 into the USB port of a separate computer. The computer card 110 is optional.

Referring to Fig. 2, the digital identity device 105 includes a microprocessor identity device 205 (further illustrated in Fig. 4), one or more memories 210, and one or more communication interfaces 215. The communication interfaces 215 couple the microprocessor identity device 205 to the memories 210.

[illegible][illegible]

credit cards' information, one or more bank accounts' information, an incorporation name, a date and a place of incorporation, one or more corporate officers, one or more corporate partners, or one or more D.B.A. names.

The second memory 210b includes an operating system 225. The operating system 225 binds the digital identity data 220 to the microprocessor identity device 205 by encoding the digital identity data 220 with passwords input by an owner of the digital identity device 105. The digital identity data 220 is encoded by an algorithm that uses the microprocessor identity information 230. The operating system 225 is secure by using commercially available encryption methods. In an alternate embodiment, the operating system 225 encrypts and stores other types of information in the memories 210. This information may be, for example, the digital identity device 105 owner's medical information or the digital identity device 105 owner's medical history. The operating system 225 also validates one or more passwords of the digital identity device 105, and one or more external systems 100 which request information from the digital identity device 105. The operating system 225 also authenticates the digital identity device 105 to the external systems 100. The operating system 225 also regulates the flow of information to and from the digital identity device 105. In an alternate embodiment, the operating system 225 is programmed to perform functions within the capabilities of the microprocessor identity device 205 of the digital identity device 105.

The microprocessor identity information 230 is bound to the digital identity data 220 by the operating system 225. The microprocessor identity information 230 provides a shortcut reference to the digital identity data 220 of the digital identity device 105. The microprocessor identity information 230 is used in the validation and authentication of external systems 100 to secure the privacy of electronic data exchange and transactions of the system 100. The

microprocessor identity information 230 serves as a surrogate for the digital identity data 220. The microprocessor identity information 230 tags all electronic transmissions with regard to the microprocessor identity device 205.

5 The communication interfaces 215 couple the memories 210 to the microprocessor identity device 205, via one or more printed circuits on the computer card 110. The communication interfaces 215 include address, data, and control electrical lines. There is a first communication interface 215a and a second communication interface 215b. The first communication interface 215a couples the first memory 210a to the microprocessor identity device 205.
10 The second communication interface 215b couples the second memory 210b to the microprocessor identity device 205.

To extract the identity of the system 100, an "Identity" or similar instruction is issued to the microprocessor identity device 205. The microprocessor identity device 205 responds by returning the microprocessor identity information 230. The microprocessor identity information 230 is returned in two or four registers. The microprocessor identity information 230 is retrieved using a single instruction or command.
15

In an alternate embodiment, the microprocessor identity device 205 is a component of a computer. The microprocessor identity device 205 identifies the computer where it resides. The microprocessor identity device 205 acts as a property tag of the computer. The microprocessor identity device 205 may also act as a property tag for other components of the computer, for example, a hard disk, a zip drive, and a sound card. The content of the components are encrypted with the microprocessor identity information 230. The integrity of the computer is set up using a security structure defined by the operating system of the computer. The operating system of the computer allows the components of the computer to work together.
20
25

Referring to Fig. 3, in an alternate embodiment, the digital identity device 105 includes the microprocessor identity device 205, a memory 310, and a communication interface 215c. The memory 310 is erasable and non-volatile to store information when the power is off to the system 100. The memory 310 is any commercially available NVRAM memory. The memory 310 includes the digital identity data 220 and the operating system 225. The digital identity data 220 is etched onto the memory 310 by an external microprocessor. The communication interface 215c electrically couples the memory 310 to the microprocessor identity device 205 through one or more printed circuits, etched on the computer card 110.

In an alternate embodiment, the memory 310 is external to a housing of the microprocessor identity device 205. The memory 310 is, for example, the Sony memory stick available from Sony, Inc. The contents of the memory 310 are encrypted using the microprocessor identity information 230 as a parameter of encryption. The contents of the memory 310 are secure and can only be read by authorized digital identity devices 105.

In an alternate embodiment, the digital identity device 105 is a single computer chip. The digital identity device 205 houses the microprocessor identity device 205 with the microprocessor identity information 230. The digital identity device 205 also houses the memory 310 with the digital identity data 220. The digital identity device 205 also houses the memory 310 with the operating system 225.

Referring to Fig. 4, the microprocessor identity device 205 is a microprocessor component 405. The microprocessor component 405 includes the microprocessor identity information 230. The microprocessor component 405 is any commercially available microprocessor unit. The microprocessor identity information 230 is etched onto the microprocessor component 405 using any conventional etching method. The microprocessor identity

information 230 is etched at the time the microprocessor component 405 is etched.

Referring to Fig. 5, in an alternate embodiment, the microprocessor identity device 205 includes a microprocessor component 505, a memory 510, and one or more communication interfaces 515. The microprocessor component 505 is any commercially available microprocessor unit, for example, the low power Reduced Instruction Set Computing (RISC) processor available from a variety of U.S. or Japanese manufacturers.

The memory 510 is programmable, non-erasable, and read-only. The memory 510 is any commercially available memory, such as Programmable Read-Only Memory (PROM). The memory 510 includes the microprocessor identity information 230. The microprocessor identity information 230 is etched onto the memory 510 using any commercially available PROM programming device.

The communication interfaces 515 electrically couple the microprocessor component 505 and the memory 510. The communication interfaces 515 include address, data, and control electrical lines.

Referring to Fig. 6, in another alternate embodiment, the microprocessor identity device 205 includes a microprocessor component 605. The microprocessor component 605 is any commercially available microprocessor unit, for example, such as the StrongARM RISC SA-1110 available from Intel, Inc. The microprocessor component 605 is specially manufactured to further include an on-die PROM memory 610. The memory 610 includes the microprocessor identity information 230. The microprocessor identity information 230 is etched onto the memory 610 using any standard means for programming. The microprocessor identity information 230 is etched at the time of manufacturing of the microprocessor component 605.

Referring to Fig. 7, in an alternate embodiment, the computer card 110

is a Universal Identity Card (UID) 705. The UID 705 is the size of a standard credit card. The digital identity device 105 is embedded in the circuitry of the UID 705. The digital identity device 105 supplies intelligence to the UID 705 via the microprocessor identity device 205. The UID 705 includes a display area 715, one or more user keys 720, and a connector 725. The display area 715 is an LCD display. The display area 715 includes a graphics area 730 and an alphanumeric area 735. Current technology allows the display area 715 to display both graphics and alphanumeric data. The display area 715 is used to display, for example, photos, thumb prints, driver's license information, social security numbers, financial information from banks, and such other data as may be deemed appropriate in the future. The user keys 720 are used to enter information or user options. The information or user options that are entered include, for example, organizer type information such as appointments, phone numbers, and address book information. The connector 725 connects the UID 705 to one or more computers or systems 100. The connector 725 is a set of fins. In an alternate embodiment, the connector 725 may be pins, sockets, or other suitable connecting means appropriate to the computers or systems 100 it is being connected to. The connector 725 utilizes common connector standards such as PCMCIA, Universal Serial Bus (USB) and RS232. The UID 705 is any card used to access personal computers, ATMs, and other public transaction devices for electronic transactions. The digital identity device 105 validates systems 100 that request information from the UID 705. The digital identity device 105 stores relevant microprocessor identity information 230 or digital identity data 220 of the systems 100 to validate the systems 100 requests. The digital identity device 105 of the UID 705 also authenticates itself to other systems 100 that request information.

In an alternate embodiment, the display area 715 may be touch-sensitive and capable of inputting information, similar to the technology used by the Palm Pilot IIIxe by Palm, Inc..

Referring to Fig. 8, in an alternate embodiment, the computer card 110 is a Corporate Identity Card 805. The Corporate Identity Card 805 is any commercially available computer card. The Corporate Identity Card 805 has the digital identity device 105 on-board. The Corporate Identity Card 805 includes a set of electrical fins 815 and a connector 820. The connector 820 connects the digital identity device 105 to the electrical fins 815. The electrical fins 815 couple the Corporate Identity Card 805 to a main computer bus. The electrical fins 815 are, for example, fins or other suitable connecting means. In a preferred embodiment, there is a single Corporate Identity Card 805 for a corporation. The Corporate Identity Card 805 validates all digital transactions of the corporation. The Corporate Identity Card 805 authenticates the corporation in all transactions to one or more systems 100.

In an alternate embodiment, the computer card 110 is a computer, such as a Personal Digital Assistant (PDA) like the Palm Pilot IIIxe available from Palm, Inc.. The computer card 110 hosts the digital identity device 105. The computer card 110 uses the microprocessor identity device 205 for its computer functions. The digital identity device 105 may be, for example, in the form of a modified FlashCard. The FlashCard may be a form of NVRAM with PROM (Programmable Read-Only Memory).

In an alternate embodiment, documents in a computer are encrypted using the microprocessor identity information 230 or the digital identity data 220. Only by using the microprocessor identity information 230 or the digital identity data 220 can the documents be decrypted. This is known as a symmetric cryptographic system.

Referring to Fig. 9, a system 900 for registering and authenticating digital identities devices 105 include one or more systems 100, a Global Registry of Digital Identity Devices (GRID) 905, and one or more communication links 910 to the Internet.

5 The systems 100 include a digital identity device 105. In a preferred embodiment, there is a first system 100a with a first digital identity device 105a and a second system 100b with a second digital identity device 105b. The first system 100a and the second system 100b reside in separate computers. Each system 100 has unique digital identity data 220 and unique
10 microprocessor identity information 230.

 The GRID 905 is a computer. The GRID 905 includes a database 915 and a digital identity device 105c. The database 915 stores microprocessor identity information 230 and digital identity data 220 for all systems 100. The database 915 is formed by each digital identity device 105 registering with the
15 GRID 905 using the communication links 910 to the Internet. The digital identity device 105c verifies and authenticates all communications between the systems 100. The GRID 905 is the universal keeper of all digital identity devices 105. If a digital identity device 105 is lost, the information within the digital identity device 105 is secure. Only the registered owner of the digital
20 identity device 105 can extract the information within the digital identity device 105. Lost digital identity devices 105 are mailed to the administrator of the GRID 905 and are returned to the owner. The GRID 905 has minimal low security information that is not encrypted, such as name and address tied to the external markings of the digital identity devices 105 or to the
25 microprocessor identity devices 205, to enable this function.

 The communication links 910 couple the GRID 905 and the systems 100 to the Internet. The communication links 910 are only necessary when there is an exchange of information between the systems 100 and/or the GRID 905.

In a preferred embodiment, the communication links 910 are Internet connections. There is a first communication link 910a coupling the first system 100a to the Internet, a second communication link 910b coupling the second system 100b to the Internet, and a third communication link 910c coupling the GRID 905 to the Internet. The systems 100 are coupled through the Internet directly. In an alternate embodiment, the systems 100 are coupled to the Internet via computers that host the digital identity devices 105.

Upon acquisition of the systems 100, the respective owners enter unique digital identity data 220 to the digital identity device 105. The digital identity data 220 is entered directly onto the digital identity device 105 using the system 100 or by attaching the system 100 to an external computer and using communication links 910. A user of the system 100 determines the digital identity data 220 necessary to identify the owner of the system 100. The user of the system 100 also determines levels of security for the system 100. The system 100 transmits the digital identity data 220 and the microprocessor identity information 230 via the communication links 910 to the GRID 905 via the Internet. An administrator of the GRID 905 verifies the digital identity data 220 provided by the owners of the system 100. The database 915 stores the digital identity data 220 and the microprocessor identity information 230 of the system 100. The GRID 905 may be used by the system 100 as a backup to the digital identity data 220 and the microprocessor identity information 230. This backup is useful for restoring the digital identity information 220 in case of loss of the system 100, a hard reset, or inadvertent erasure of data.

Referring to Fig. 10, a system 1000 for transactions between digital identities includes one or more systems 100 and one or more communication links 1005. There is a first system 100a and a second system 100b coupled by the communication link 1005. The communication link 1005 is any communication means, for example, an Internet connection, keycard access, or

an ATM digital identity device jack. The digital identity data 220 of the systems 100 include information that are particular to the individuals or corporations involved in the transactions. The individual digital identity devices 105 allows only authorized access to the digital identity data 220 of each system 100. The authorized access to the digital identity data 220 of each system 100 is relayed to the GRID 905 during set up of the database 915. The system 100 is used for transactions, such as, Internet retailing, banking, business-to-business, electronic permission, and secure communications. This would be similar to the process of establishing an account with a bank or establishing credit with a financial institution. The digital identity devices 105 contain information for the transactions, for example, bank balances, credit card balances, payments, electronic travelers checks, and security transactions.

In an alternate embodiment, the transaction may be electronic communication, for example, e-mail. A digital signature encrypts the e-mail. The digital signature may be the microprocessor identity information 230. The systems 100 authenticate the e-mail by decrypting the e-mail using the previously stored security access maintained in the GRID 905 or in the digital identity device.

Referring to Fig. 11A, a system 1100 for licensing software includes a first licensee computer 1105a, a vendor computer 1110, and a connection 1115. The connection 1115 couples the licensee computer 1105 to the vendor computer 1110. The connection 1115 is the Internet.

The first licensee computer 1105a includes a first microprocessor identity device 205a and a digital identity device 105. The digital identity device 105 includes a second microprocessor identity device 205b. The microprocessor identity devices 205 include the microprocessor identity information 230 for their respective microprocessor identity devices 205.

The vendor computer 1110 includes a software program 1120 and a software key database 1140. The software program 1120 is distributed via the Internet. In an alternate embodiment, the software program 1120 is distributed via a CD-ROM or some other media.

5 The software key database 1140 is generated by the vendor computer 1110 and contains one or more license keys 1125 available for installation. Each license key 1125 has a one-to-one relationship with a copy of the software program 1120. After installation, the license key 1125 binds the microprocessor identity information 230 of the first licensee computer 1105a in
10 the software key database 1140. In an alternate embodiment, the microprocessor identity information 230 is encrypted using an algorithm that uses the license key 1125 in the arguments.

 The connections 1115 are any data connection used to transfer information between computers, for example, an Internet connection. In an
15 alternate embodiment, the connection 1115 is a high-speed data connection.

 Referring to Fig. 11B, in an alternate embodiment, the system 1100 further includes a second licensee computer 1105b and an internal network connection 1150. The second licensee computer 1105b includes a third microprocessor identity device 205c. The second licensee computer 1105b is
20 coupled to the first licensee computer 1105a by the internal network connection 1150.

 In an alternate embodiment, the second licensee computer 1105b is directly coupled to the connection 1115. The second licensee computer 1105b operates through a gateway controlled by the first licensee computer 1105a.

25 Referring to Fig. 12, a method 1200 for licensing software includes: in step 1205, initiating the software installation; in step 1210, sending information; in step 1215, verifying the license status; in step 1220, binding

information; and in step 1225, completing the installation. The method 1200 may be used to license software to a computer, an individual, or a corporation.

In step 1205, the first licensee computer 1105a initiates the installation process by downloading the software program 1120 via the connection 1115.

5 The installation process is automatically initiated by the downloading process.

In an alternate embodiment, the first licensee computer 1105a initiates the installation process by running a setup program within the software program 1120.

10 In step 1210, the first licensee computer 1105a sends the microprocessor identity information 230 of the microprocessor identity device 205a and the license key 1125 to the vendor computer 1110 via the connection 1115. The license key 1125 issues to the first licensee computer 1105a during step 1205. The software program 1120 licenses to the first licensee computer 1105a.

15 In an alternate embodiment, the software license key 1125 issues on the software media or a container for the software media.

In an alternate embodiment, the first licensee computer 1105a sends the microprocessor identity information 230 of the microprocessor identity device 205b and the license key 1125 to the vendor computer 1110 via the connection 1115. The software program 1120 licenses to the digital identity device 105.

20 In step 1215, the vendor computer 1110 verifies the microprocessor identity information 230 from the first licensee computer 1105a. The vendor computer 1110 confirms the presence of the license key 1125 in the software key database 1140 to determine if the license key 1125 is valid. The vendor computer 1110 further determines if the license key 1125 is already coupled in
25 the software key database 1240. If coupled, there may be a breach of the licensing agreement. The vendor computer 1110 requests alternate microprocessor identity information 230 from the first licensee computer 1105a and establishes multiple links to the license key 1125. In an alternate

embodiment, the vendor computer 1110 halts the method 1200 if the license key 1125 is coupled. In an alternate embodiment, the vendor computer 1110 chooses to halt the method 1200 and take actions outside this automated licensing method 1200.

5 In step 1220, the vendor computer 1110 binds the license key 1125 to the microprocessor identity information 230. The software key database 1140 associates the microprocessor identity information 230 to the license key 1125. The microprocessor identity device 205a is encrypted using the license key 1125. In an alternate embodiment, the license key 1235 is encrypted using the
10 microprocessor identity device 205a.

 In step 1225, the first licensee computer 1105a completes the installation of the software program 1120. The first licensee computer 1105a also stores the bound microprocessor identity information 230 and the license key 1125 from step 1220.

15 In an alternate embodiment, if the licensee agreement allows, a second licensee computer 1105b installs the software program 1120 from the first licensee computer 1105a using the method 1200. The software key database 1140 associates the microprocessor identity information 230 of the microprocessor identity device 205a, 205b, or 205c to the license key 1125. The
20 association of the license, whether to the first licensee computer 1105a or the digital identity device 105, is determined by the licensing terms of the software program 1120.

 In an alternate embodiment, the method 1200 applies to other types of intellectual property, such as MP3 music, which runs on computers with
25 microprocessor identity devices 205.

 Referring to Fig. 13, a method 1300 for de-licensing software includes: in step 1305, de-installing software; in step 1310, verifying the license status; in step 1315, un-binding identity device and software license key; and in step

1320, completing de-installation. The method 1300 is the logical reverse of the method 1200.

5 In step 1305, the first licensee computer 1105a starts the de-installation of the software program 1120. The software program 1120 is de-installed using a standard de-installation program supplied by the vendor. The first licensee computer 1105a transmits the license key 1125 and the microprocessor identity information 230 to the vendor computer 1110 via the connection 1115.

10 In an alternate embodiment, the first licensee computer 1105a sends the microprocessor identity information 230 of the microprocessor identity device 205b and the license key 1125 to the vendor computer 1110 via the connection 1115.

15 In an alternate embodiment, the second licensee computer 1105b sends the microprocessor identity information 230 of the microprocessor identity device 205c and the license key 1125 to the vendor computer 1110 via the first licensee computer 1105a.

20 In step 1310, the vendor computer 1110 verifies the binding of the license key 1125 and the microprocessor identity information 230 in the software key database 1140. If the license key 1125 and the microprocessor identity information 230 do not match the values stored in the software key database 1140, the vendor computer 1110 halts the method 1300. In an alternate embodiment, there are other corrective actions the vendor computer 1110 may take to correct an exception to its licensing agreement.

25 In step 1315, the vendor computer 1110 un-binds the license key 1125 to the microprocessor identity information 230 in the software key database 1140. The software key database 1140 un-associates the microprocessor identity information 230 to the license key 1125. The software key database 1140 leaves a blank field for the microprocessor identity information 230.

In step 1320, the vendor computer 1110 completes the reinstallation process by updating the software key database 1140. The first licensee computer 1105a removes the software program 1120.

5 In an alternate embodiment, the second licensee computer 1105b performs the method 1300 to de-install the software program 1120. The method 1300 de-installs the software from the second licensee computer 1105b, but not the first licensee computer 1105a (such as in a private network).

10 In a networked environment, the methods 1200 and 1300 are done on an individual computer basis, especially when software resides on the computers in which they are used.

Referring to Fig. 14, a method 1400 for tracking software usage includes: in step 1405, starting the software; in step 1410, creating usage information; and in step 1415, transmitting the usage information. Tracking software usage determines licensing fees by the vendor computer 1110. The
15 method 1400 assumes the first licensee computer 1105a has already performed the method 1200.

In step 1405, the first licensee computer 1105a starts and uses the software program 1120.

20 In step 1410, the software program 1120 creates usage information. The usage information may include, for example, start time, stop time, and users.

In an alternate embodiment, the usage information is stored in a file on the first licensee computer 1105a.

25 In step 1415, the first licensee computer 1105a transmits the usage information to the vendor computer 1110 via the connection 1115.

In an alternate embodiment, the first licensee computer 1105a transmits the file of the usage information when the connection 1115 is in

Although illustrative embodiments of the invention have been shown and described, a wide range of modification, changes and substitution is contemplated in the foregoing disclosure. In some instances, some features of the present invention may be employed without a corresponding use of the other features. Accordingly, it is appropriate that the appended claims be construed broadly and in a manner consistent with the scope of the invention.

Claims

What is claimed is:

- 1 1. A digital identity device for identifying legal entities, comprising:
2 a microprocessor identity device;
3 a digital identity; and
4 means for binding the microprocessor identity device to the digital
5 identity.
- 1 2. The digital identity device of claim 1, wherein the microprocessor
2 identity device comprises a microprocessor having a unique
3 microprocessor identity.
- 1 3. The digital identity device of claim 1, wherein the microprocessor
2 identity device comprises a microprocessor and a memory; and
3 wherein the memory has a unique microprocessor identity.
- 1 4. The digital identity device of claim 3, wherein the memory is
2 programmable and read-only.
- 1 5. The digital identity device of claim 4, wherein the memory is on-die or
2 off board the microprocessor.
- 1 6. The digital identity device of claim 1, wherein the digital identity is for
2 one of the group consisting of an individual and a corporation; and
3 wherein the digital identity is unique.

- 1 7. The digital identity device of claim 1, wherein the means for binding is a
2 secure operating system.
- 1 8. The digital identity device of claim 1, wherein the digital identity device
2 further comprises a computer device and means for communicating
3 between the computer device and the digital identity device.
- 1 9. The digital identity device of claim 8, wherein the computer device is a
2 computer board, a computer card, or a computer device with an
3 input/output port.
- 1 10. An apparatus for globally registering digital identity devices,
2 comprising:
3 one or more digital identity devices;
4 a database of digital identity device information; and
5 means for communications between the digital identity devices and the
6 database.
- 1 11. A method of licensing a software program to a computer, the computer
2 having a microprocessor containing identity information about the
3 computer, the method comprising the steps of:
4 a. starting the installation of the software program to the computer;
5 b. transmitting a license key and the identity information about the
6 computer to a central database;
7 c. receiving information to bind the license key to the identity
8 information;
9 d. binding the license key to the identity information in the
10 computer; and

11 e. completing the installation.

12

1 12. The method of claim 11, wherein the identity information is for one of
2 the group consisting of an individual, a computer, and a corporation;
3 and wherein the identity information is unique.

1 13. The method of claim 11, wherein the identity information resides in a
2 digital identity device.

1 14. The method of claim 11, wherein starting the installation of the
2 software program comprises any standard installation method.

1 15. The method of claim 11, wherein transmitting the license key and the
2 identity information comprises any standard communication
3 transmission method.

1 16. The method of claim 11, wherein receiving information to bind the
2 license key to the identity information comprises receiving information
3 from a central database regarding a status of the license key using any
4 standard communication reception method.

1 17. The method of claim 11, wherein binding the license key to the identity
2 information in the computer comprises using a secure operating system.

1 18. A method of de-licensing a software program to a computer, the
2 computer having a microprocessor containing identity information
3 about the computer, the method comprising the steps of:

- 4 a. starting the de-installation of the software program to the
5 computer;
6 b. transmitting a license key and the identity information about the
7 computer to a central database;
8 c. receiving information to unbind the license key to the identity
9 information;
10 d. unbinding the license key to the identity information in the
11 computer; and
12 e. completing the reinstallation.

1 19. The method of claim 18, wherein the identity information is for one of
2 the group consisting of an individual, a computer, and a corporation;
3 and wherein the identity information is unique.

1 20. The method of claim 18, wherein the identity information resides in a
2 digital identity device.

1 21. The method of claim 18, wherein starting the de-installation of the
2 software program comprises any standard de-installation method.

1 22. The method of claim 18, wherein transmitting the license key and the
2 identity information comprises any standard communication
3 transmission method.

1 23. The method of claim 18, wherein receiving information to unbind the
2 license key to the identity information comprises receiving information
3 from a central database regarding a status of the license key using any
4 standard communication reception method.

- 1 24. The method of claim 18, wherein unbinding the license key to the
2 identity information in the computer comprises using a secure operating
3 system.
- 1 25. A method of tracking software usage by a computer, the computer
2 having a microprocessor containing identity information about the
3 computer, the method comprising the steps of:
4 a. receiving a usage profile from the computer; and
5 b. storing the usage profile in a central database.
- 1 26. The method of claim 25, wherein the identity information is for one of
2 the group consisting of an individual, a computer, and a corporation;
3 and wherein the identity information is unique.
- 1 27. The method of claim 25, wherein the identity information resides in a
2 digital identity device.
- 1 28. The method of claim 25, wherein receiving a usage profile from the
2 computer comprises receiving the identity information and a usage time
3 stamp by any standard electronic communication reception method.
- 1 29. The method of claim 25, further comprising calculating a usage fee from
2 the usage profile.
- 1 30. A method of identifying an origin of electronic communication,
2 comprising tagging the electronic communication,

3 wherein the origin comprises a microprocessor containing identity
4 information about the origin, wherein tagging the electronic
5 communication comprises encrypting the electronic communication
6 using the identity information in the encryption algorithm, and wherein
7 the identity information is for one of the group consisting of an
8 individual, a computer, and a corporation; and wherein the identity
9 information is unique.

1 31. The method of claim 30, wherein the identity information resides in a
2 digital identity device.

1 32. A method of identifying property, the property having a microprocessor
2 containing identity information about the property, the method
3 comprising binding the property to the microprocessor, wherein binding
4 the property comprises binding the identity information to the property
5 using a secure operating system, wherein the identity information is for
6 one of the group consisting of an individual, a computer, and a
7 corporation; and wherein the identity information is unique.

1 33. The method of claim 32, wherein the identity information resides in a
2 digital identity device.

1 34. A method of securing one or more electronic documents, comprising
2 encrypting the documents, wherein the electronic documents are stored
3 on a computer having a microprocessor containing identity information,
4 wherein the identity information is for one of the group consisting of an
5 individual, a computer, and a corporation; and wherein the identity
6 information is unique.

1 35. The method of claim 34, wherein the identity information resides in a
2 digital identity device.

1 36. The method of claim 35, wherein encrypting the documents comprises
2 using the identity information in the encryption algorithm.

1 37. A method of licensing a software program to a computer, the computer
2 having a microprocessor containing identity information about the
3 computer, the method comprising the steps of:

- 4 a. receiving a license key and the identity information about the
5 computer into a central database;
6 b. transferring a status of the license key and the identity
7 information in the central database to the computer;
8 c. accepting the license key and the identity information; and
9 d. binding the license key to the identity information in the central
10 database.

1 38. The method of claim 37, wherein the identity information is for one of
2 the group consisting of an individual, a computer, and a corporation;
3 and wherein the identity information is unique.

1 39. The method of claim 38, wherein the identity information resides in a
2 digital identity device.

1 40. The method of claim 39, wherein receiving a license key and the identity
2 information about the computer into a central database comprises any
3 standard communication reception method.

1 41. The method of claim 40, wherein transferring a status of the license key
2 and the identity information in the central database to the computer
3 comprises looking up the status of the license key in the central
4 database.

1 42. The method of claim 41, wherein accepting the license key and the
2 identity information comprises updating the central database to include
3 the license key and the identity information.

1 43. The method of claim 42, wherein binding the license key to the identity
2 information in the central database comprises linking the license key to
3 the identity information.

1 44. A method of de-licensing a software program to a computer, the
2 computer having a microprocessor containing identity information
3 about the computer, the method comprising the steps of:
4 a. receiving a license key and the identity information about the
5 computer into a central database;
6 b. transferring a status of the license key and the identity
7 information in the central database to the computer;
8 c. accepting the license key and the identity information; and
9 d. unbinding the license key to the identity information in the
10 central database.

1 45. The method of claim 44, wherein the identity information is for one of
2 the group consisting of an individual, a computer, and a corporation;
3 and wherein the identity information is unique.

1 46. The method of claim 45, wherein the identity information resides in a
2 digital identity device.

1 47. The method of claim 46, wherein receiving a license key and the identity
2 information about the computer into a central database comprises any
3 standard communication reception method.

1 48. The method of claim 47, wherein transferring a status of the license key
2 and the identity information in the central database to the computer
3 comprises looking up the status of the license key in the central
4 database.

1 49. The method of claim 48, wherein accepting the license key and the
2 identity information comprises updating the central database to exclude
3 the license key and the identity information.

1 50. The method of claim 49, wherein unbinding the license key to the
2 identity information in the central database comprises de-registering the
3 license key to the identity information.

100

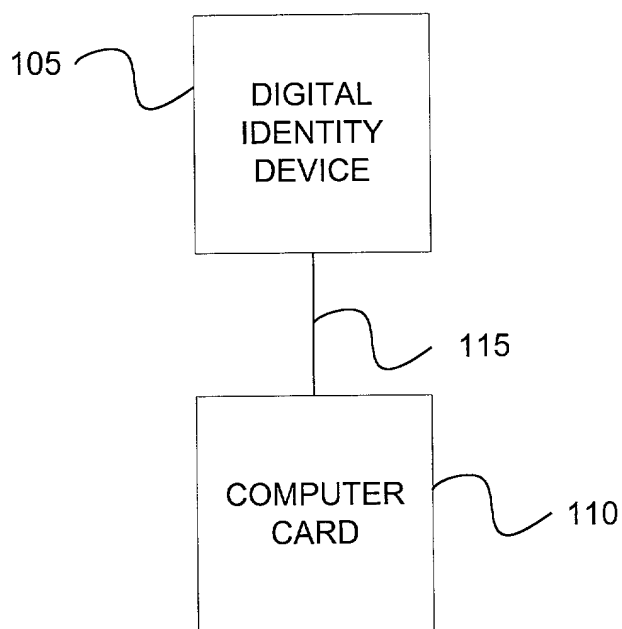


Fig. 1

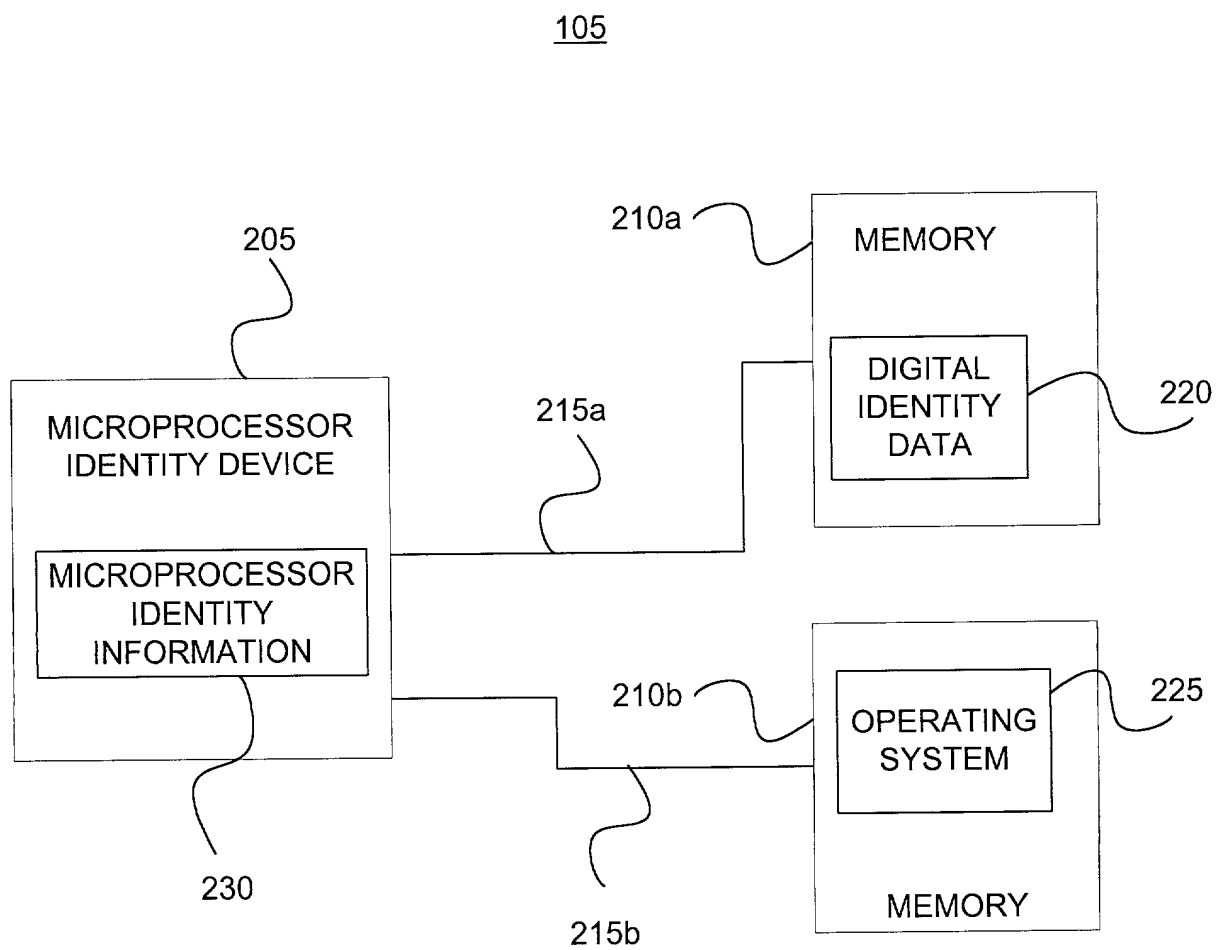


Fig. 2

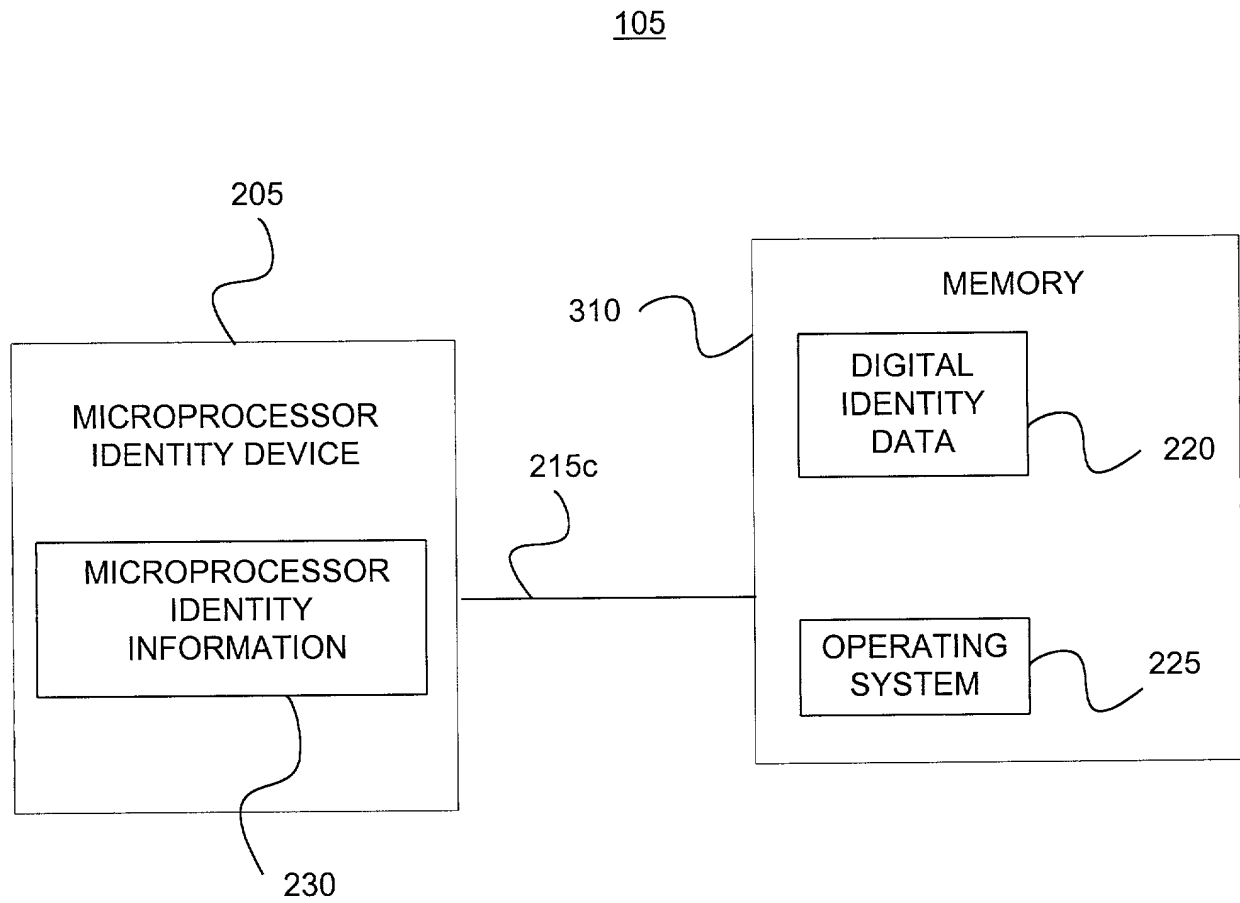


Fig. 3

205

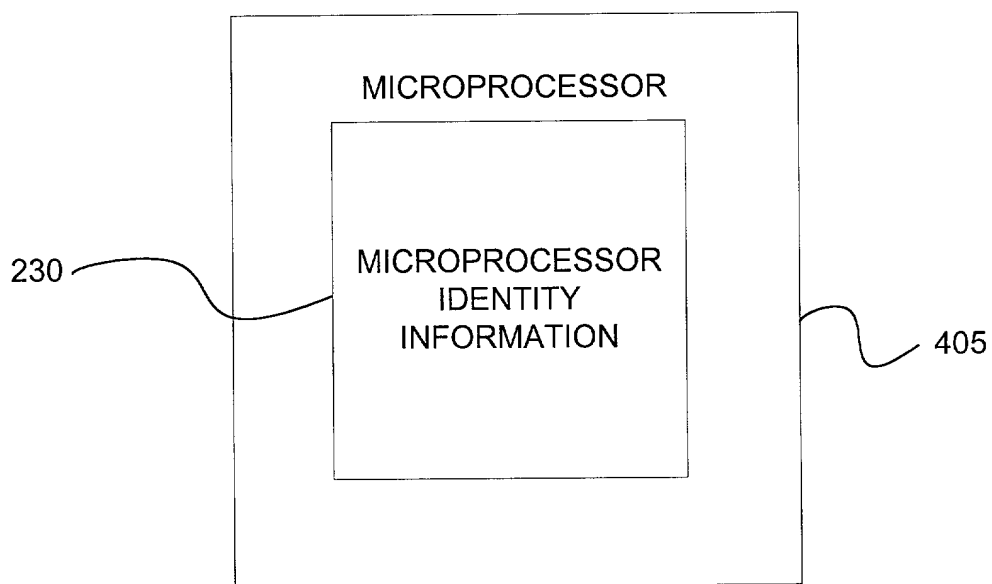


Fig. 4

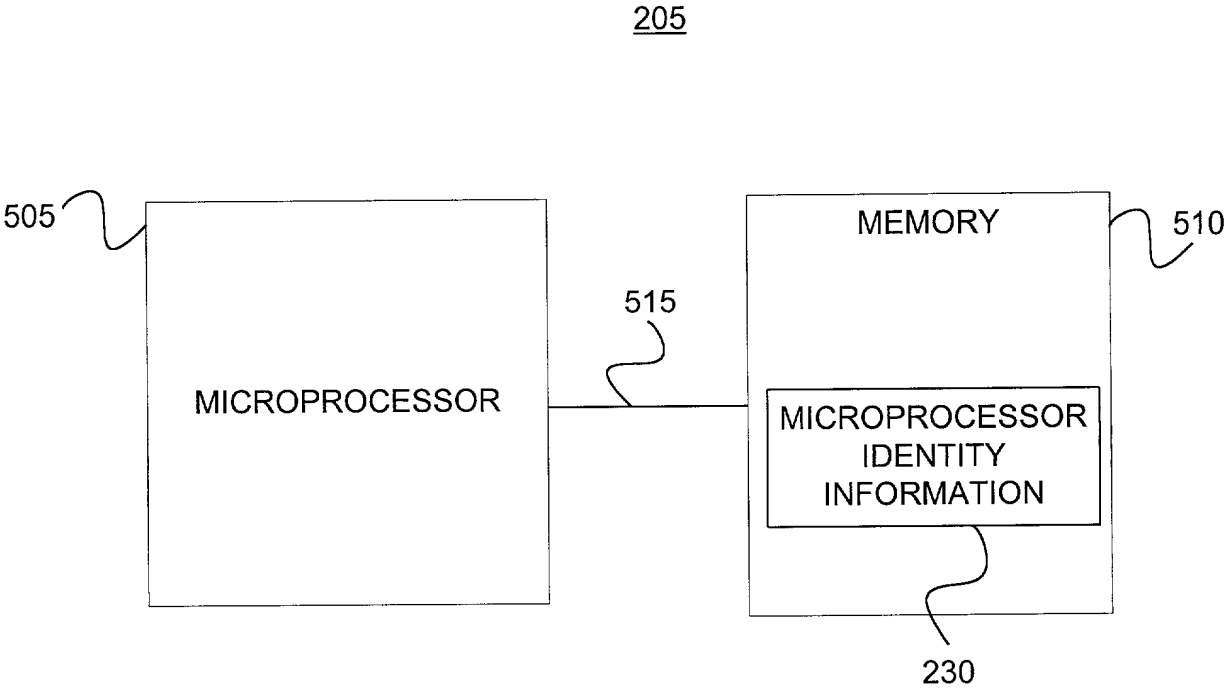


Fig. 5

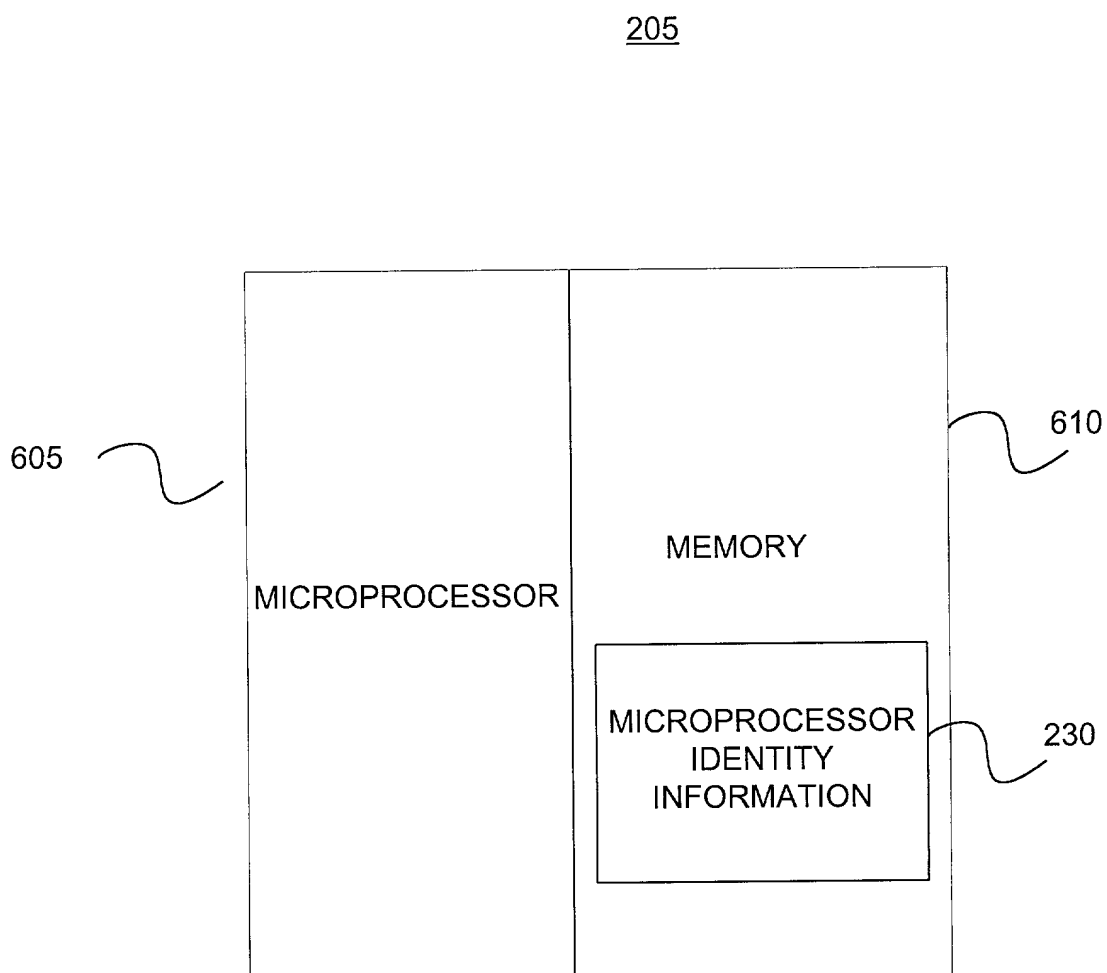


Fig. 6

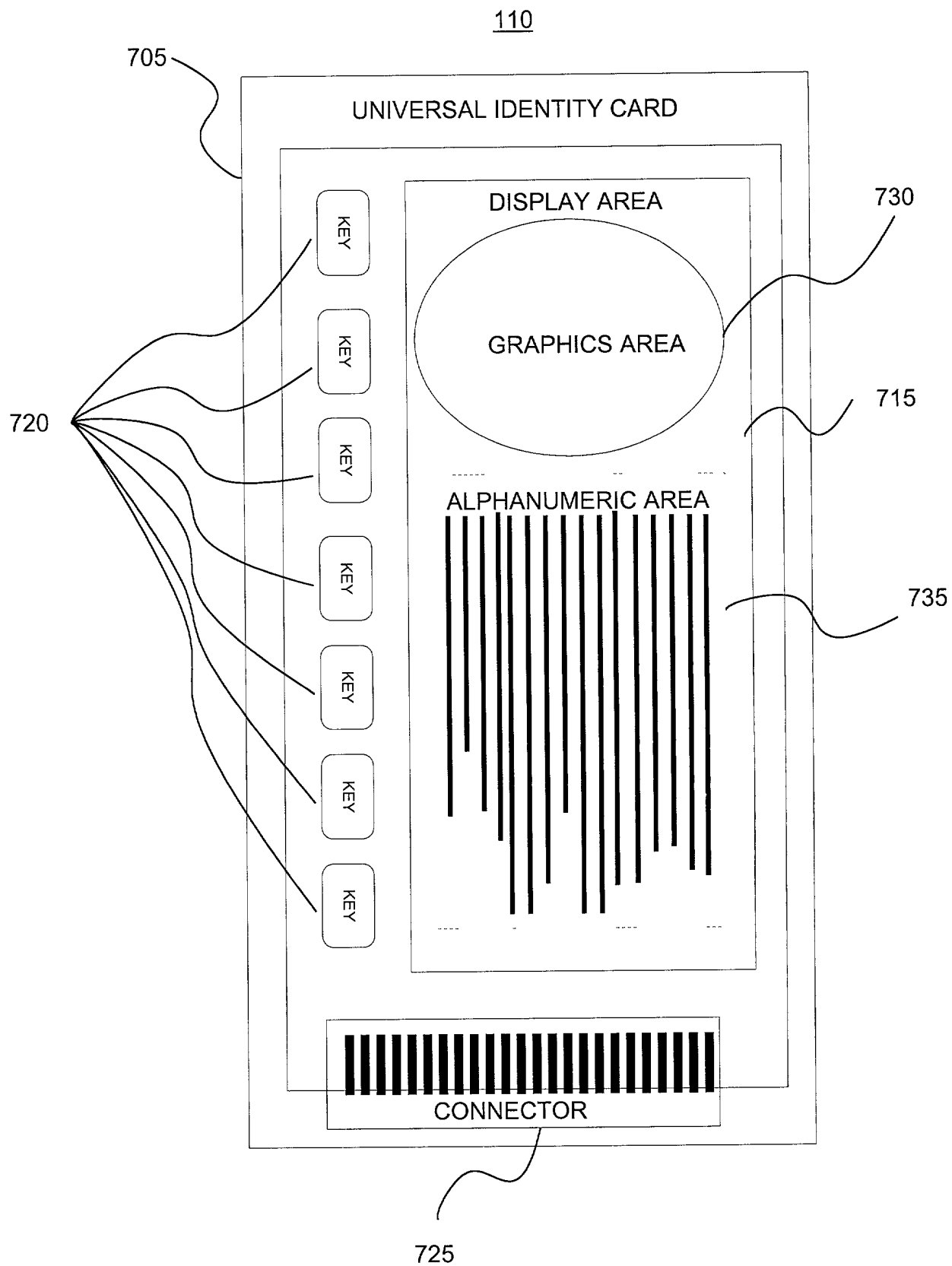


Fig. 7

110

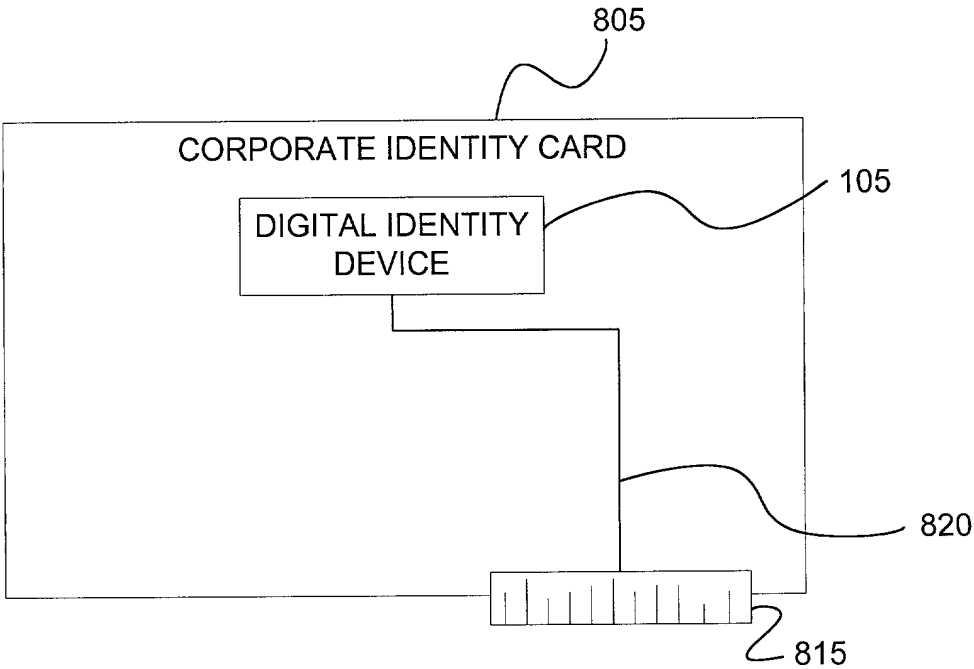


Fig. 8

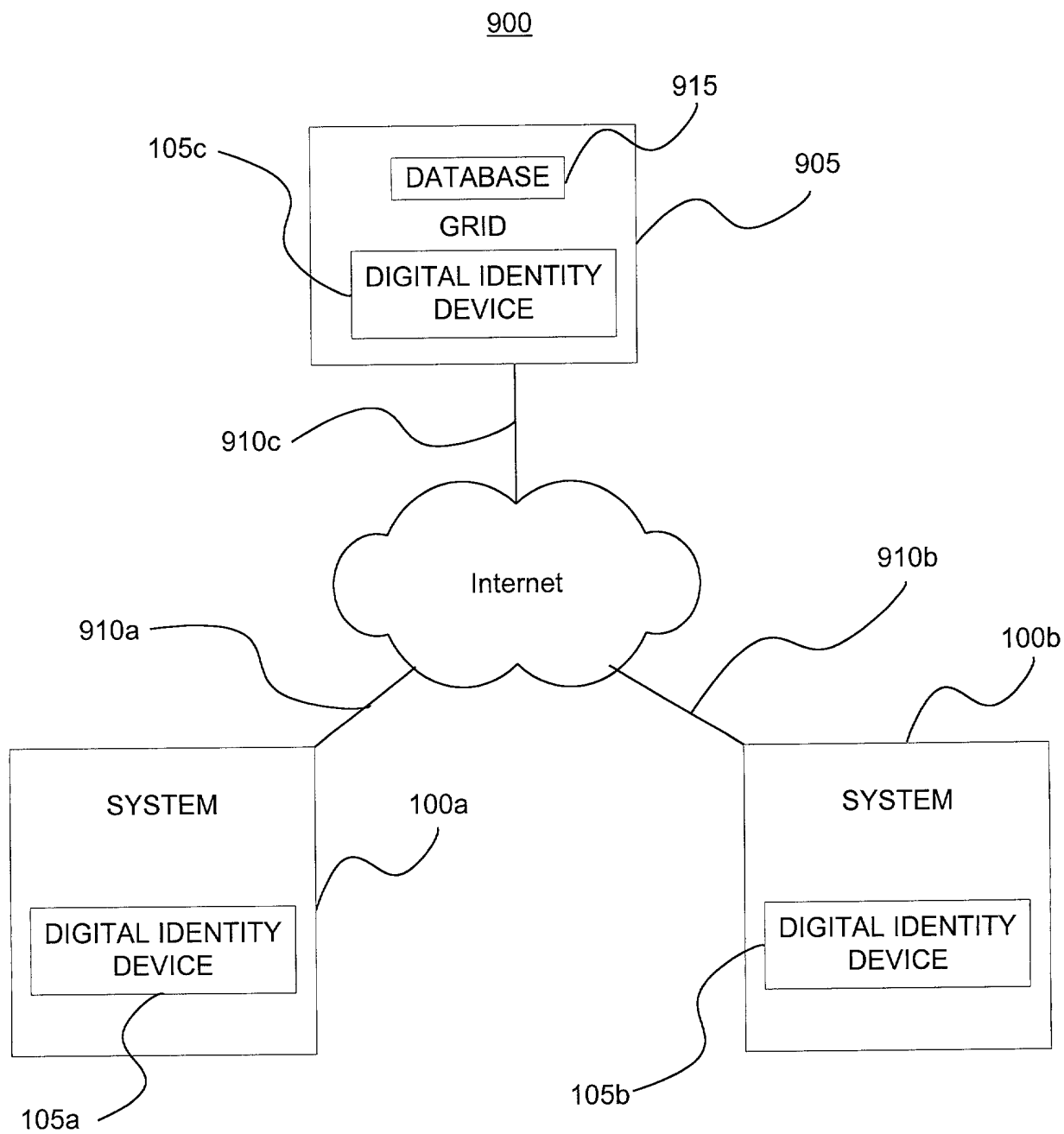


Fig. 9

1010

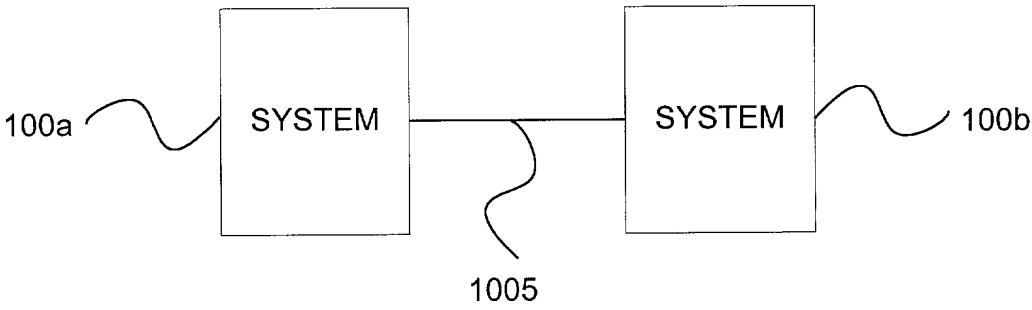


Fig. 10

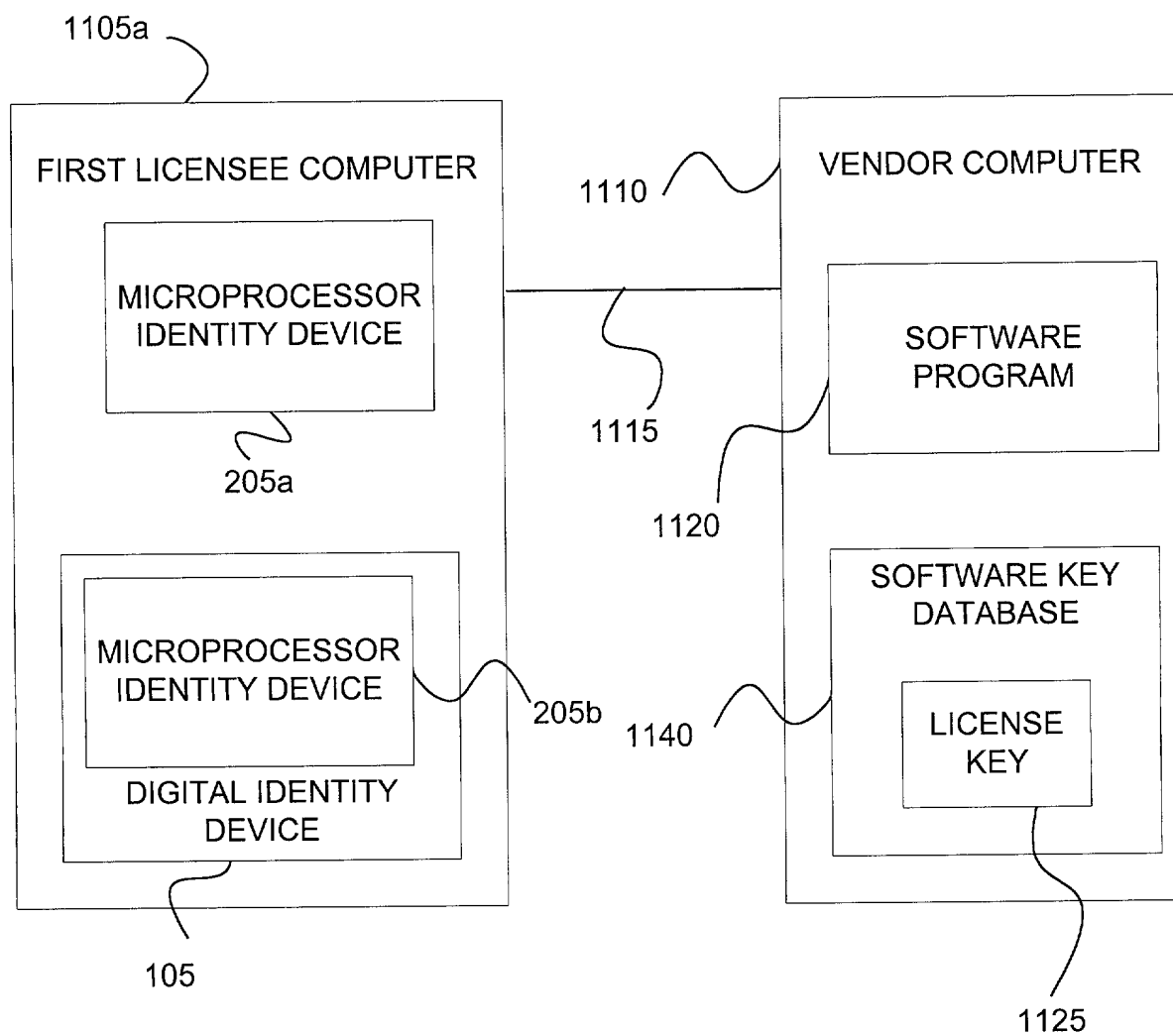
1100

Fig. 11A

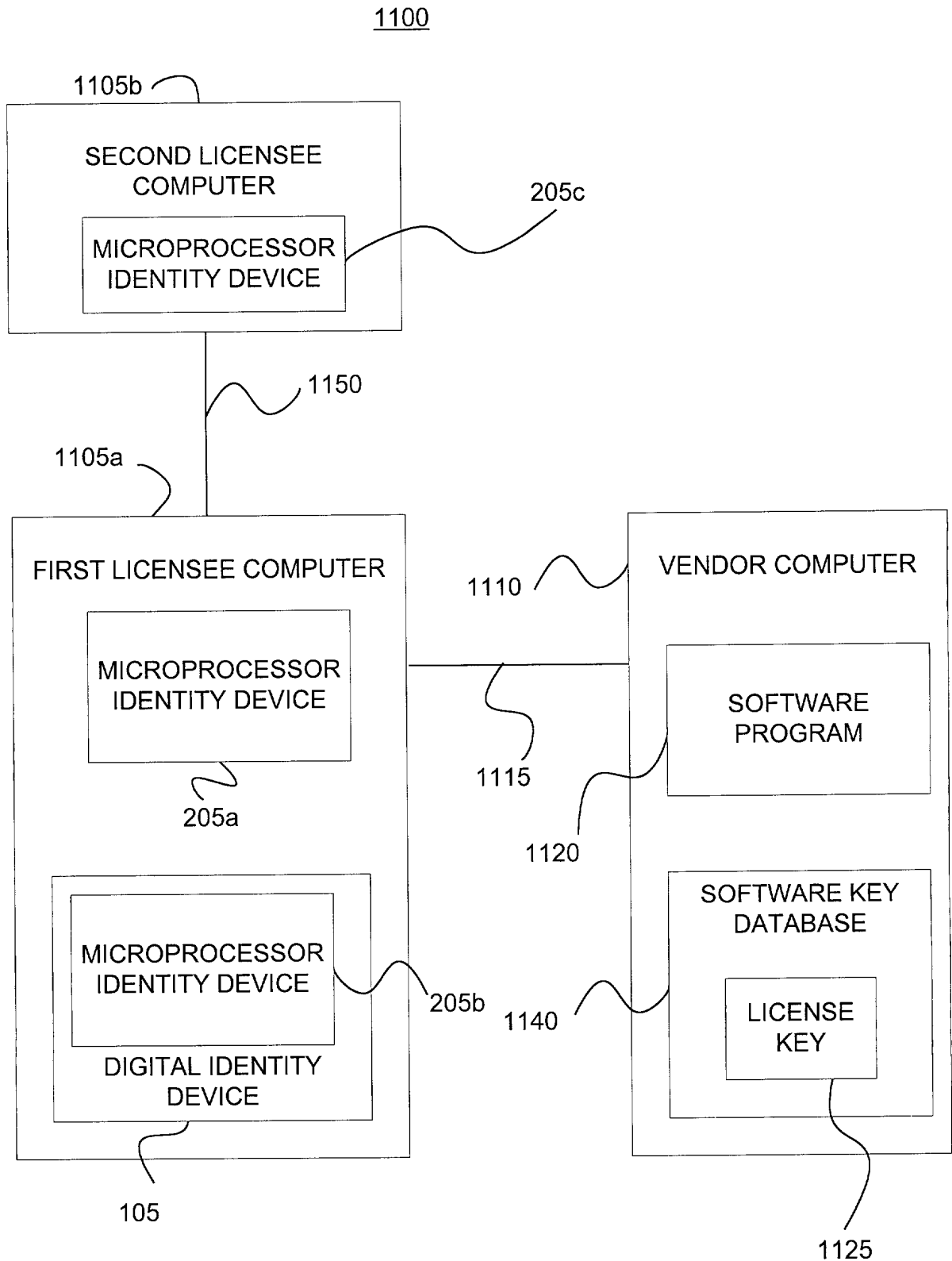


Fig. 11B

1200

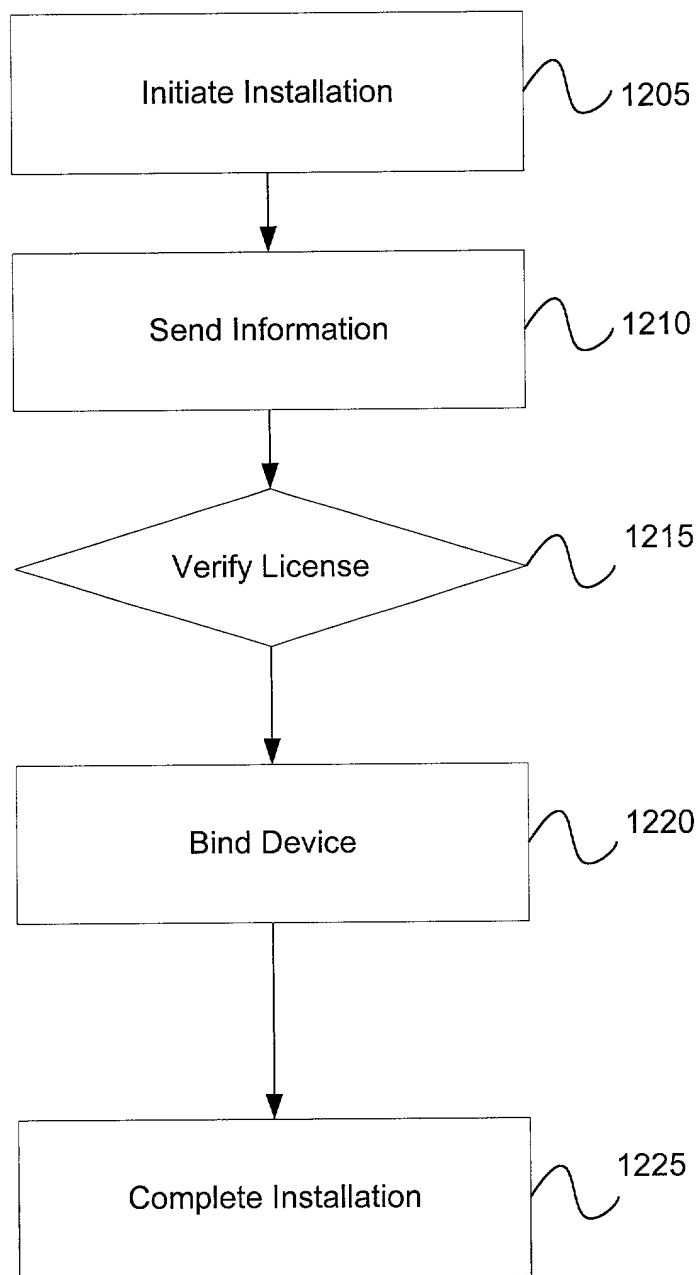


Fig. 12

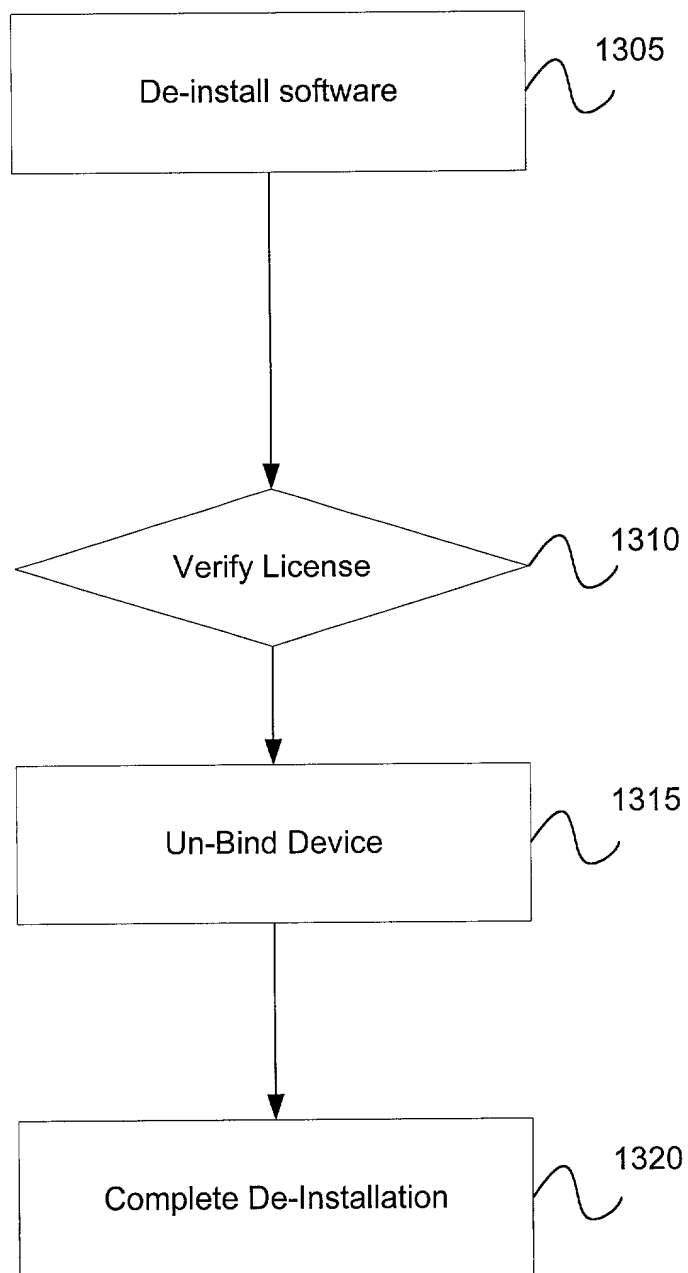
1300

Fig. 13

1400

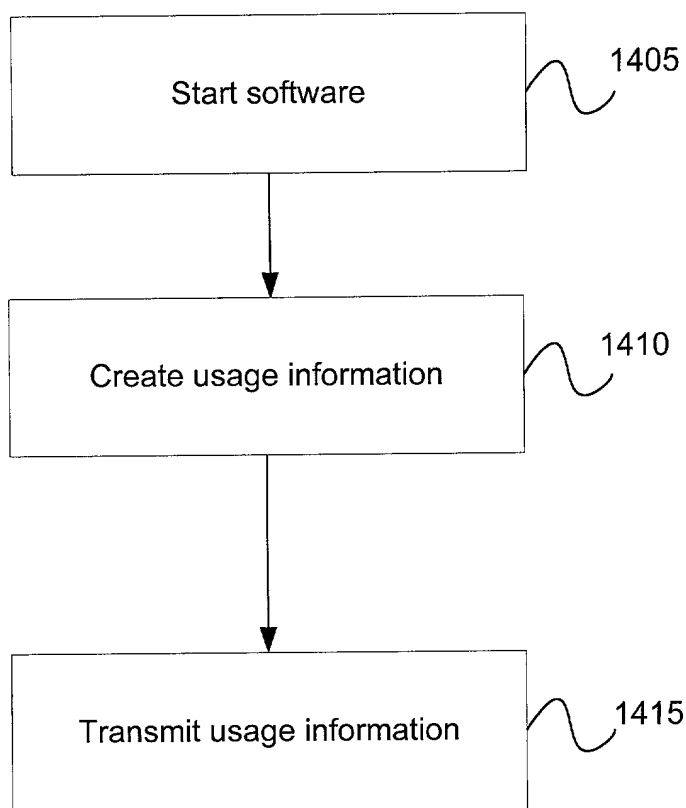


Fig. 14

DECLARATION

As the below-named inventor, I declare that:

My residence, post office address, and citizenship are as stated below next to my name.

I believe that I am the original, first, and sole inventor of the subject matter which is claimed, and for which a patent is sought on the application entitled:

DIGITAL IDENTITY DEVICE

the specification of which: (check one)

_____ is attached hereto.
_____ was filed on _____
under Attorney's Docket Number _____
as Application Serial No. _____
and was amended on _____ (if applicable).

I have reviewed and understand the contents of the above-identified specification, including the claims.

I acknowledge the duty to disclose to the United States Patent and Trademark Office all information known to me to be material to patentability, as defined in Title 37, Code of Federal Regulations, § 1.56.

I claim the benefit under Title 35, United States Code, §120 of any United States application(s) listed below, and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, § 112, I acknowledge the duty to disclose to the United States Patent and Trademark Office all information known to me to be material to patentability as defined in Title 37, Code of Federal Regulations, § 1.56 which became available between the filing date of the prior application and the national or PCT international filing date of this application.

60/179,989
Application

February 3, 2000
Filing Date

Status (serial no. pending)

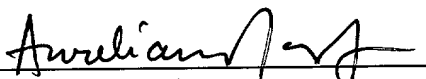
POWER OF ATTORNEY: As a named inventor, I hereby appoint the following attorneys and/or agents to prosecute this application and transact all business in the U.S. Patent and Trademark Office connected therewith.

| | | | |
|------------------------|-----------------|--------------------|-----------------|
| Jeffrey M. Becker | Reg. No. 35,442 | Mark E. McBurney | Reg. No. 33,114 |
| James R. Bell | Reg. No. 26,528 | David L. McCombs | Reg. No. 32,271 |
| Michael S. Bush | Reg. No. 31,745 | David M. O'Dell | Reg. No. 42,044 |
| Randall E. Colson | Reg. No. 40,566 | Michael D. Pegues | Reg. No. 38,993 |
| Michael A. Davis, Jr. | Reg. No. 35,488 | Phillip B. Philbin | Reg. No. 35,979 |
| Ruben C. DeLeon | Reg. No. 37,812 | Brandi W. Sarfatis | Reg. No. 37,713 |
| Timothy Headley | Reg. No. 31,765 | David O. Simmons | Reg. No. 43,124 |
| Warren B. Kice | Reg. No. 22,732 | | |
| Michael Balconi-Lamica | Reg. No. 34,291 | | |
| Todd Mattingly | Reg. No. 40,298 | | |

I request that all correspondence be directed to Tim Headley, Haynes and Boone, L.L.P., 1000 Louisiana Street, Suite 4300, Houston, Texas 77002-5012.

All statements made of my own knowledge are true, and all statements made on information and belief are believed to be true. These statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the application or any patent issued.

Full name of inventor: Aureliano Tan, Jr.

Inventor's signature:  Date: 9-1-2000

Residence (City, State): Sugar Land, Texas

Citizenship: United States of America

Post Office Address: _____